



UNITED STATES DISTRICT COURT

for the
District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

4200 MONTGOMERY BLVD. NE, APT 209,
ALBUQUERQUE, NEW MEXICO 87109

Case No. **23mr353**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ District of _____ New Mexico _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841	Distribution and possession with intent to distribute controlled substances;
21 U.S.C. § 846	Conspiracy to distribute controlled substances;
18 U.S.C. § 2	Aiding and abetting.

The application is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jerrod Pelot, FBI Task Force Officer

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephonically sworn and electronically signed (specify reliable electronic means).

Date: February 14, 2023

City and state: Albuquerque, New Mexico

Judge's signature

Laura Fashing, U.S. Magistrate Judge

Printed name and title

[illegible]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF:
4200 MONTGOMERY BLVD. NE, APT 209,
ALBUQUERQUE, NEW MEXICO 87109

Case No. _____

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, Jerrod Pelot, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 4200 Montgomery Blvd. NE, Apt 209, Albuquerque, New Mexico 87109, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I have been a Task Force Officer with the Federal Bureau of Investigation ("FBI") since May 2016. As such, I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and I am empowered by law to conduct investigations and to make arrests for criminal offenses, to include those enumerated in 18 U.S.C. § 2516.

3. I have been a law enforcement officer since 2008. I am currently a Detective with the Albuquerque Police Department ("APD"). I am also assigned to the FBI's Transnational Organized Crime- West Task Force (TOC-WEST), which investigates large scale transnational criminal organizations.

4. During my time in law enforcement, I have received hundreds of hours of formal training in the areas of gang and drug investigations from the federal, state, and local law enforcement agencies.

5. During my law enforcement career, I have participated in hundreds of investigations involving narcotics violations, firearms violations, fugitives, property crimes, money laundering/financial crimes, gang crimes/activities and the investigation of criminal enterprises. My investigative experience includes, but is not limited to, conducting surveillance, interviewing subjects, targets, witnesses, writing affidavits for and executing search and arrest warrants, acting in an undercover capacity, supervising cooperating sources, managing undercover agents, issuing administrative subpoenas, analyzing phone records, analyzing financial records, and utilizing data derived from pen registers and trap and trace devices.

6. Through my training and experience, I am familiar with the methods and means used by individuals and drug trafficking organizations to purchase, transport, store, and distribute controlled substances. I am also familiar with how those individuals and organizations hide the profits generated from their criminal activities.

7. I have been involved in an ongoing investigation regarding the distribution of controlled substances, specifically methamphetamine and fentanyl, by Gilbert SANDOVAL and others, known and unknown. Since the investigation's inception, I, as well as other Special Agents and Task Force Officers with the FBI, and law enforcement officials from other agencies have

obtained information regarding the illegal drug trafficking activities of Gilbert SANDOVAL and others (the "SUBJECTS").

8. I make this affidavit based upon my own personal knowledge, which is substantially derived from my participation in the investigation, as well as that of fellow agents and officers who have participated in the investigation. In addition, I have developed information I believe to be reliable from additional sources including:

- a. Information provided by Task Force Officers ("TFO"), Special Agents ("SA"), and Intelligence Research Specialists (IRS) of the FBI, and other law enforcement officials ("agents"), including oral and written reports that I have received directly or indirectly from said investigators;
- b. Results of physical surveillance conducted by agents during the investigation;
- c. A review of driver's license and automobile registration records;
- d. Records from commercial databases; and
- e. Records from the National Crime Information Center ("NCIC").

2. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

FEDERAL CHARGES RELEVANT TO THIS INVESTIGATION

3. I believe there is probable cause that the SUBJECTS have committed, are

committing, and will continue to commit offenses involving violations of:

- a. 21 U.S.C. § 841 – Distribution and possession with intent to distribute controlled substances;
- b. 21 U.S.C. § 846 – Conspiracy to distribute and possess with intent to distribute controlled substances; and
- c. 18 U.S.C. § 2 – Aiding and abetting.

EVIDENCE SOUGHT DURING SEARCH

9. Based on my training, experience and participation in this and in similar investigations, I believe that individuals involved in illegal trafficking of controlled substances often conceal evidence of their drug trafficking activities in their residences and businesses, or the residences of friends or relatives, and in surrounding areas to which they have ready access such as garages, carports and outbuildings. They also conceal evidence in vehicles, including vehicles outside of their residences and businesses, so that they have ready access to it and so that they can hide it from law enforcement, including law enforcement officers executing search warrants at their residences or businesses. Evidence also may be found in other areas to which a drug dealer has ready access, such as rented storage areas and safety deposit boxes, or buried underground on their property. This evidence, which is discussed in detail in the following paragraphs, includes controlled substances, paraphernalia for weighing, packaging and distributing controlled substances, other contraband, records, documents, as well as evidence of drug transactions, proceeds from drug sales, and valuables obtained from proceeds.

10. Individuals involved in illegal drug trafficking of controlled substances often keep quantities of controlled substances on their person, in their residences, garages, outbuildings, storage areas, carports and yards, in their businesses, in the residences of friends or relatives, in their vehicles, in off-site storage facilities, and in other areas to which they have ready access.

11. Individuals involved in drug dealing commonly use certain paraphernalia to package and prepare controlled substances for distribution. The paraphernalia includes, but is not limited to, packaging materials (such as plastic baggies, wrapping paper, cellophane, condoms, and film canisters) and scales to weigh controlled substances. Drug dealers commonly store these items on their person, in their residences, in their businesses, in their residences of friends or relatives, in their vehicles, and in other areas to which they have ready access.

12. Drug traffickers often maintain records of their transactions in a manner similar to the record keeping procedures of legitimate businesses. Even after the drugs are sold, documentary records are often maintained for long periods of time, even years, to memorialize past transactions, the status of accounts receivable and accounts payable, and the names and telephone numbers of suppliers, customers and co-conspirators. These records may be maintained on paper, in the form of business and personal ledgers and diaries, calendars, memoranda, pay/owe sheets, IOUs, miscellaneous notes, money orders, customer lists, and telephone address books. These records can reflect names, addresses and/or telephone numbers of associates and co-conspirators, the sale and purchase of controlled substances including precursors, customer lists, and amounts of money owed to the trafficker by customers and by the trafficker to his/her suppliers.

13. Drug traffickers often travel domestically and internationally to facilitate their trafficking. Evidence of foreign and domestic travel by persons engaged in illegal drug trafficking includes travel itineraries, airline tickets, receipts, passports, and visas. These items are stored by drug dealers on their person or in their business, residences and surrounding garages, outbuildings, carports and yards, the residences of relatives and in cars. Many of these items are accessible via the internet and can be downloaded and saved on the computer or other digital media and on storage media.

14. Drug traffickers often use storage facilities for drugs and other items related to trafficking that are at a location away from their residences and businesses. These off-site storage facilities are often commercial storage lockers and rooms. These locations are often used to store or hide drugs, contraband, money and other valuables. Drug traffickers often keep documents and other items tending to show the existence of other stored drugs, contraband, money and other valuables in areas such as storage facilities. Those documents and other items include rental agreements, receipts, keys, notes and maps specifically concerning off-site storage rooms, lockers, and safety deposit boxes. This evidence may be found on their person or in their businesses, residences and surrounding garages, outbuildings, carports and yards, the residences of friends or relatives, and cars. This type of documentation can be stored on digital media and concealed virtually anywhere.

15. Other evidence of transportation, ordering, possession and sale of drugs can include the following: telephone bills to show numbers called by the drug dealers (and hence potential

associates), overnight mail receipts, bank statements, deposit and withdrawal slips, savings books, investment statements, loan statements, other financial institution statements, and federal and state tax returns. The above items are stored by drug dealers on their person or in their business, residences and surrounding garages, outbuildings, carports and yards, the residences of friends or relatives, and cars. This type of documentation can be stored on digital media and concealed virtually anywhere.

16. Drug traffickers usually sell their product for cash. Because large quantities of drugs can sell for thousands of dollars at the wholesale level, dealers may have thousands of dollars in cash on hand both as proceeds of sales and to purchase supplies/inventory. In addition, drug dealers often have other assets generated by their drug business, or purchased with cash earned, such as precious metals and stones, jewelry, real estate, vehicles, and other valuables.

17. Individuals involved in drug dealing often try to legitimize these profits from the sale of drugs. To accomplish this goal, drug traffickers may utilize foreign and/or domestic banking institutions and their attendant services, real estate and businesses, both real and fictitious. They also try to secret, transfer and conceal the money by (a) placing assets in names other than their own to avoid detection while maintaining control, (b) laundering money through what appears to be a legitimate business or businesses, (c) hiding the money in their homes, safes and safety deposit boxes, and/or (d) using the money to buy assets which are difficult to trace. This evidence is useful in a criminal prosecution, and it also is useful in identifying real and personal

property that can be seized and forfeited by the government under existing laws. Documentation concerning this type of activity can be stored on digital media and concealed virtually anywhere.

18. Evidence of significant, unexplained income of drug dealers, or for the acquisition and concealment of money and assets of drug sales, can be found on banking and investment account statements, credit card account statements, canceled checks, money orders, deposit slips, check and savings books, business and personal ledgers, accounting records, safe deposit box records and keys, federal and state tax records, rental receipts, rental agreements, utility bills, overnight mail receipts, telephone bills, loan statements, records reflecting ownership of real or personal property (such as deeds of trust or vehicle registration, insurance, and ownership information), vehicle and property rental records, lease and purchase agreements, and canceled mail. These records can be maintained on paper, but also can be maintained as electronic data on computers and other digital media. The above items are typically kept by drug dealers on their person or in their businesses, residences and surrounding garages, outbuildings, carports, and yards, the residences of friends or relatives, and vehicles.

19. The use of digital media, including smartphones, tablets, cellular phones, and digital devices, has become part of everyday life. This is also true for drug traffickers. Information stored in electronic form on all of the above-devices can provide evidence of drug trafficking. Drug traffickers frequently use some or all of these devices to communicate with co-conspirators, customers, sources of supply, and others involved in the drug trade. These communications include, but are not limited to, phone calls, text messages, SMS (Short Message Service)

messaging, MMS (Multimedia Messaging Service) messaging, social media posts and messaging, and smartphone application messaging services. Smartphones, tablets, cellular phones, and digital devices are frequently capable of storing messages, emails, social media communications, and communications made over smartphone applications. The content of these communications will often provide evidence of drug trafficking. Numbers stored on a telephone (such as Caller ID lists reflecting recently received calls, speed dial lists of names and/or telephone numbers, and logs of outgoing and incoming calls) can provide evidence of who the drug dealer is calling, and thus the identity of potential associates.

20. Drug traffickers often take, or cause to be taken, photographs and/or videos of themselves, their associates, their property and their drugs. They usually maintain these photographs and/or videos on their person or in their businesses, residences or cars, on computers, or in the residences of friends or relatives. Smartphones, tablets, cellular phones, digital cameras, and other digital devices, often have the capability to take still photos and videos and save them indefinitely on the device's storage medium. Drug traffickers frequently use these devices to take their photographs and videos.

21. Drug traffickers often maintain firearms and ammunition on their person or in their homes, businesses or cars to protect themselves and their drugs and their drug profits. They also may maintain indicia of firearms such as receipts for firearms and ammunition, boxes for firearms and ammunition, firearms cleaning supplies, and instruction manuals and other documentation for firearms and ammunition.

22. I know that weapons (including rifles, shotguns, and handguns) are tools of the trade for drug traffickers, who often keep firearms in close proximity to themselves, and their product and proceeds, to protect them from other drug traffickers and law enforcement.

23. Drug traffickers often conceal evidence of drug dealing in vehicles outside of their residences for ready access and to prevent detection and seizure by officers executing search warrants at their residences. This evidence, which is discussed in detail in the preceding paragraphs, includes controlled substances, indicia such as packing documents and electronic storage devices (and their contents,) evidence tending to show the distribution of drugs (such as IOUs, pay-owe sheets, ledgers, lists of names and numbers, telephone address books, etc.), digital devices such as cellular/mobile/smart telephones and tablets (and their contents), and counter-surveillance devices.

24. Drug traffickers often utilize digital video surveillance systems. A digital video surveillance system is a surveillance system that is capable of capturing images, videos, and audio that can be compressed, stored or sent over communication networks. I know that it is common for digital surveillance systems to contain storage media that allow for 30 days or more of camera footage to be stored on the system. Digital video surveillance systems can be used for nearly any environment, including a commercial business or residence. I know that drug traffickers make use of video surveillance systems to monitor who is approaching their residence and assess whether the person presents a threat to the trafficker's drugs or drug proceeds. Drug traffickers also utilize surveillance equipment to obtain advance notice when law enforcement arrives to hide or destroy

evidence of criminal activity. However, given the constant recording that occurs with a digital surveillance system, it is also common that the digital video surveillance system will also depict evidence of the residents' drug trafficking activities and conversations related to drug trafficking.

25. Documents showing who owns, occupies, or controls the location being searched also show who is responsible for the items found on the premises, including contraband and other evidence seized. Documents and items showing the identity of the persons owning, residing in or controlling the area being searched include, but are not limited to, utility and telephone bills, canceled envelopes and correspondence, outgoing answering machine messages, tax returns, keys, deeds and mortgage receipts. These documents may also be produced on computers, downloaded from online accounts or scanned into digital format and stored on computers and related digital media.

26. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, smartphones, tablets, server computers, and network hardware. The term "digital media" includes personal digital assistants (PDAs), smartphones, tablets, BlackBerry devices, iPhones, iPods, iPads, digital cameras, and cellular telephones. The term "storage media" includes any physical object upon which electronic data can be recorded, such as hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media or digital medium. Collectively, the terms "computer," "digital media," and "storage media" are referred to as "electronic media."

27. A list of items agents seek authority to seize is in Attachment B.

ELECTRONIC MEDIA AND FORENSIC ANALYSIS

28. As described above and in Attachment B, this application seeks permission to search for evidence and records that might be found on the PREMISES, in whatever form they are found. Much of the evidence and records described in the paragraphs above, and in Attachment B, can also be produced and/or stored on electronic media. For this reason, I submit that if a computer, digital medium, or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer, digital medium, or storage medium. Thus, the warrant applied for would authorize the seizure of electronic media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. *Necessity of seizing or copying entire electronic media.* In most cases, a thorough search of a premises for information that might be stored on electronic media often requires the seizure of the physical electronic media and later off-site review consistent with the warrant. In lieu of removing electronic media from the premises, it is sometimes possible to make an image copy of electronic media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the electronic media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence

takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. Electronic media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the electronic media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of electronic media formats that may require off-site reviewing with specialized forensic tools.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying electronic media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the computer or entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

31. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the

ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

- c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.
- d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or

alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

- e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.
- f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint

for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

- g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the PREMISES and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

- h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the PREMISES and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

PROBABLE CAUSE

A. APD Encounter at the PREMISES

32. On January 29, 2023, Albuquerque Police Department (“APD”) Field Officers J. Lerma (#7344) and V. Padilla (#6387) were dispatched to Apartment 209 of the Atrium Apartments, located at 4200 Montgomery Blvd. NE in Albuquerque, New Mexico.

33. A concerned neighbor (“CS-1”), advised officers that the man living in Apartment 209, later identified as Gilbert SANDOVAL, was a drug dealer. CS-1 explained that he/she had observed drug paraphernalia around the apartment constantly, as well as people using illegal narcotics. CS-1 further witnessed multiple young women, who he/she believed to be runaways, visiting the apartment with garbage bags. When CS-1 asked why the women were there, the

women responded that the people living in the apartment would help them for a “trade.” Based on my training and experience in other investigations, I believe that the use of “trade” here refers to an exchange of sex for drugs.

34. CS-1 added that he/she had seen the residents within Apartment 209 wearing bulletproof vests and placing suspicious bags—which CS-1 believed to be narcotics—into their vehicle.

35. APD officers checked SANDOVAL through the National Criminal Information Center (“NCIC”) for warrants and confirmed that SANDOVAL was wanted on a felony warrant for his arrest out of the state of Arizona. SANDOVAL left the property prior to contact with officers.

B. FBI Surveillance at the PREMISES

36. Independently, agents and Task Force Officers of the FBI (collectively, “agents”) conducting an ongoing investigation into narcotics trafficking in the Albuquerque area identified SANDOVAL as a local source of supply. They obtained a photograph of SANDOVAL using public records databases. They also conducted a toll analysis showing that SANDOVAL was in direct contact with a Mexican-based source of supply.

37. Between late 2022 and early 2023, agents conducted extensive surveillance at the PREMISES. Agents were familiar with the apartment complex containing the PREMISES from prior investigations.

38. While agents could not observe the entry door of the PREMISES, they could observe both the common landing that led to the door, as well as the private balcony of the PREMISES.

39. Agents repeatedly observed SANDOVAL, among others, entering and exiting the landing outside the PREMISES and appearing on the private balcony. He appeared to remain at the PREMISES overnight.

40. In January and February 2023, agents observed SANDOVAL's vehicle in the late evening hours parked within the secured perimeter parking lot. Follow up surveillance the next morning would observe the vehicle parked in the same secured parking area.

41. The high volume of foot traffic into and out of the PREMISES (and present on the balcony) was, based on my training and experience, consistent with drug trafficking.

C. SANDOVAL's Arrest

42. On January 31, 2023, Albuquerque Police Department Officer V. Padilla (#6387) was conducting a random patrol conducting a random patrol when he observed a gray Chevrolet sport utility vehicle traveling eastbound on Menaul Blvd NE. The vehicle matched the description of a vehicle owned by SANDOVAL, and a records check confirmed that SANDOVAL was the registered owner of the vehicle. Officer Padilla followed the gray SUV.

43. SANDOVAL parked his gray SUV on private property, exited the vehicle, and entered a business. As SANDOVAL was leaving the business, officers arrested him without incident for his felony warrant.

44. SANDOVAL had a black fanny pack around his waist. A search revealed that the fanny pack contained a white crystal-like substance, as well as multiple individual Ziploc baggies and a small scale.

45. Officers field-tested the white crystal-like substance using a Narcotics Identification System. The substance tested presumptively positive for the presence of methamphetamine.

46. Officer Padilla then Mirandized SANDOVAL. SANDOVAL stated he understood his rights and agreed to speak with Officers. SANDOVAL stated the fanny pack and its contents belonged to him and that he was “guilty.” SANDOVAL added that he knew better and that he was “screwed.”

47. A female passenger inside of the vehicle was identified as Jerika LORENZEN. Officers released the vehicle and SANDOVAL’s phone to her at his request. LORENZEN was released.

48. Agents spoke with another neighbor (“CS-2”), who informed them that suspicious activity has continued at the PREMISES, including a high volume of foot traffic. CS-2 added that “young girls” continue to frequent the apartment.

49. Agents also contacted CS-1 to ask about activity after SANDOVAL’s arrest. CS-1 confirmed that people continue to visit the apartment frequently, including young women.

50. Both CS-1 and CS-2 confirmed that SANDOVAL lived in the PREMISES prior to his arrest.

D. Conclusion

51. Despite SANDOVAL's arrest, agents believe that the PREMISES nonetheless contains evidence of drug trafficking for two primary reasons.

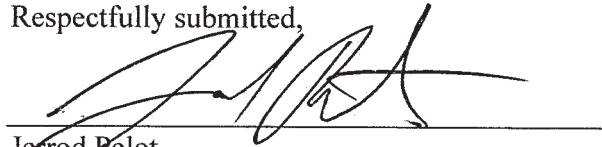
52. First, other suspected drug traffickers frequented the PREMISES during agents' surveillance. SANDOVAL's co-conspirators may remain in the apartment and use it to further their drug trafficking activities. This possibility is consistent with CS-2's account of continued traffic into and out of the apartment.

53. Second, while LORENZEN or co-conspirators may have removed actual controlled substances after SANDOVAL's arrest in an attempt to conceal his activities, in my training and experience drug traffickers often forget to remove documents, drug packaging, and other less obvious forms of evidence. Bank records, credit card statements, travel records, and even drug ledgers are often left behind at a target's primary residence.

CONCLUSION

54. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,



Jerrod Pelot
Task Force Officer
Federal Bureau of Investigation

Electronically signed and telephonically sworn
on February 14, 2023:



LAURA FASHING
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 4200 Montgomery Blvd. NE, Apt 209, Albuquerque, New Mexico 87109, hereinafter "PREMISES," further described as an apartment with a north-facing balcony on the second floor of a larger tan apartment complex.

The search of the above PREMISES shall include the search of the entire residence, all attached and unattached garages and storage areas/containers (including mailboxes and trash cans) on the PREMISES, and all persons located in the PREMISES in or on which the items to be seized could be concealed. The search shall also include all vehicles parked at, or in front of, the PREMISES that have an apparent connection to Gilbert SANDOVAL, including any vehicle owned and/or operated by SANDOVAL, or registered to SANDOVAL. Connection to the vehicle may be established by evidence that SANDOVAL owns, operates, and/or has or had access to any vehicle parked at or in front of the PREMISES. Evidence includes prior law enforcement observation, vehicle registration, witness statement(s), or an ignition key found on the PREMISES.

ATTACHMENT B

Property to be seized

- I. All records, information, and evidence relating to violations of 21 U.S.C. §§ 841 and 846, as well as 18 U.S.C. § 2, those violations involving Gilbert SANDOVAL and occurring after January 1, 2022, including:
 1. Controlled substances, including, but not limited to, methamphetamine, heroin, cocaine, and marijuana.
 2. Drug paraphernalia, including but not limited to, scales, packaging materials, items for packaging and handling drugs.
 3. Large amounts of currency, financial instruments, precious metals, jewelry and other items of value and/or proceeds of drug transactions.
 4. Any and all drug customer lists, drug records, dealers lists, or any notes containing the individual names of such persons, telephone numbers, addresses of these customers or dealers, and any corresponding records of accounts receivable, money paid or received, drugs supplied or received, or cash received to pay for controlled substances or intended to pay for controlled substances.
 5. Telephone and address books or notes containing telephone numbers and addresses of co-conspirators.
 6. Telephone toll records for homes and/or businesses owned or controlled by suspected co-conspirators, or other communication devices used by them and/or their drug trafficking associates.

7. Messages, notes, correspondence, and/or communications between drug trafficking associates.
8. Indications of ownership or control of said premises and/or other premises used in unlawful drug trafficking activity, including but not limited to, utility bills, cancelled checks, or envelopes and deeds or leases.
9. Indications of ownership or control over any vehicles located at the place to be searched, including but not limited to, titles, registrations, gas receipts, repair bills and keys belonging to that vehicle.
10. Records, receipts, bank statements and records, money drafts, letters of credit, money orders and cashier's checks received, passbooks, bank checks, safe deposit box keys, vault keys, safes and other items evidencing the obtaining, secreting and/or concealment, and or expenditures of money.
11. Any and all financial or other instruments evidencing placement of assets in the names other than the names of the drug traffickers themselves.
12. Books, records, receipts, diaries, notes, ledgers, airline tickets, cashier's checks, money orders and other papers relating to the transportation, ordering, sale and distribution of controlled substances and the outstanding debts and collections from controlled substances that have been distributed.
13. Photographs or videos of the drug traffickers, their co-conspirators and the property and assets purchased with drug proceeds.
14. Other financial records, which may include airline ticket receipts, credit card receipts, rental car receipts and luggage tags reflecting points of travel.

15. Firearms and ammunition, including but not limited to handguns, rifles, shotguns and automatic weapons.
16. Digital video surveillance systems, including the associated storage media.
17. Any and all computers, digital media, and storage media that reasonably appear to contain some or all of the records, information, and/or evidence described in Attachment B.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer, digital media, or storage media; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “digital media” includes personal digital assistants (PDAs), smartphones, tablets, BlackBerry devices, iPhones, iPods, iPads, digital cameras, and cellular telephones.

The term “storage media” includes any physical object upon which electronic data can be recorded, such as hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media or digital medium.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, smartphones, tablets, server computers, and network hardware.

This warrant authorizes a review of all electronic media seized pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The warrant also authorizes a review of all electronic media for evidence of who used, owned, or controlled the

electronic media at the time the things described in this warrant were created, edited, or deleted. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, law enforcement may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual who is found at the PREMISES and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.